# 物理複製困難ハードウェア ID の抽出手法に関する研究

修士学位論文要約（平成30年 3 月）

# 物理複製困難ハードウェア ID の抽出手法に関する研究

鈴木 麻奈美
指導教員：青木 孝文

# An Extraction Method for Phsycally Unclonable Hardware ID

Manami SUZUKI
Supervisor: Takafumi AOKI

This paper presents efficient methods for extracting hardware ID from Physically Unclonable Functions (PUFs). The basic idea of the proposed method is to handle PUF responses as multiple values and then to debias them in the binary form that can be available for common fuzzy extractors. As a result, the entropy and stability of resulting hardware ID are significantly improved. This paper also shows the advantages of the proposed methods in terms of the required hardware cost and the authentication success rate via two experiments with simulated and actual responses of PUFs.

## 1. はじめに

近年の LSI 再加工・解析技術の発展に伴い，LSI の不正な再利用や模造品・偽造品による被害が急増している．LSI の不正品に対する既存対策として，LSI に ID を与えて認証を行う手法がある．しかし，現状における LSI の ID に関する問題として ID そのものの模造・偽造があげられる．そこで，LSI 上に実装可能な物理複製困難関数 (PUF: Physically Unclonable Function) に基づく LSI の ID 生成が注目されている．PUF は LSI の制御不能な製造ばらつき（半導体素子のドライブ能力や配線遅延など）を利用することで LSI の各個体に固有かつ第三者に予測不能な値を生成する．PUF の出力値（レスポンス）を LSI ごとの ID の生成や格納の際に用いることで，リバースエンジニアリングなどの攻撃に対しても安全に認証を行うことができる．

PUF に基づく ID 生成において，PUF に必要とされる重要な性質の一つに安定性が挙げられる．安定性とは，ある PUF に対して同じ入力を繰り返したときに得られるレスポンスがどれだけ同一であるかを表す指標である．PUF から安定した ID を抽出するために誤り訂正符号 (ECC: Error Correction Code) を用いたファジー抽出器 (FE：Fuzzy Extractor) [1] が用いられる．PUF の安定性が低い場合，時間（電力）のコストが大きい強力な誤り訂正が必要となるだけでなく，PUF のサイズ（ハードウェアコスト）も増大する．PUF に求められるもう一つの重要な性質として予測不可能性がある．予測不可能性とは PUF レスポンスを推定することの困難さを表す指標である．予測不可能性を満たすために最も重要な性質の一つとして一様性があげられる．多くの場合，PUF の一様性はレスポンスにおける 0 と 1 の出現確率の偏り（バイアス）として与えられる．レスポンスのバイアスが大きい PUF に FE を用いた場合，FE が生成する公開データから ID に関する秘密情報が漏洩することが知られている．しかし，バイアスのない理想的な PUF を作ることは困難であるため，デバイアシングとよばれる PUF レスポンスのバイアスを軽減する手法を FE と組み合わせる手法が提案されている [2]．

PUF の安定性と予測不可能性を向上させる手法として，レスポンスの多値化がある [3]．しかし，多値レスポンスは，対応するデバイアシング手法や FE が報告されていないため，応用先が限られるという問題点があった．

そこで，本論文では PUF の多値レスポンスに対応する多値デバイアシングを提案し，PUF の ID 生成の高効率化を行う．

## 2. 3 値デバイアシング

PUF は多数のセルからなり，各セルの出力によってレスポンスが生成される．セルはレスポンスを生成する試行の度に出力が常に 0 か 1 の定数を出力する定数セルと，試行ごとに 0 か 1 のどちらかを出力するランダムセルに分類できる．各セルに値を割り当てることで 3 値レスポンスを生成することができる．

提案する 3 値デバイアシング手法は入力を 3 値レスポンス，出力を 2 値レスポンスとすることで既存

表 1　3 値デバイアシング

| Enrollment | | | Reconstruction | | |
|---|---|---|---|---|---|
| input | output | | input | | output |
| $t_{2i}t_{2i+1}$ | $y_i$ | $d_i$ | $t'_{2i}t'_{2i+1}$ | $d_i$ | $y'_i$ |
| 0 0 | discard | 0 | 0 - | 1 | 0 |
| 1 1 | discard | 0 | 1 - | 1 | 1 |
| $r$ $r$ | discard | 0 | $r$ $r$ | 1 | 1 |
| 0 1 | 0 | 1 | $r$ 0 | 1 | 1 |
| $r$ 1 | 0 | 1 | $r$ 1 | 1 | 0 |
| 0 $r$ | 0 | 1 | - - | 0 | discard |
| 1 0 | 1 | 1 | | | |
| $r$ 0 | 1 | 1 | | | |
| 1 $r$ | 1 | 1 | | | |

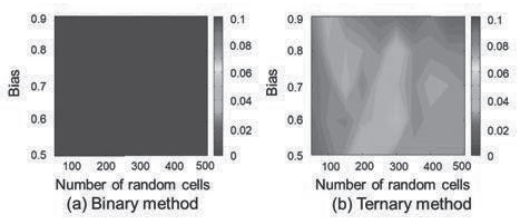


図 1　各デバイアシング手法によって得られるバイアスの最悪値

の FE に組み合わせることができる．提案手法では入力を 2 桁ごとのブロックに区切り，その値に応じて 0 か 1 の値を出力するか，入力情報を破棄することでバイアスの小さなレスポンスを抽出する．定数 (0, 1) セル，ランダムセルに割り当てる値をそれぞれ 0，1，$r$ とする．表 1 に提案手法の入出力関係を示す．ここで，FE 登録時と復元時における 3 値レスポンスとデバイアシング後のレスポンス，デバイアシングデータの $i$ 番目の値をそれぞれ $t_i$，$t'_i$，$y_i$，$y'_i$，$d_i$ とする．提案手法では，FE 復元時における入力の誤りを一部訂正することが可能であるため，デバイアシング後のレスポンスの安定性を向上可能である．また，高いエントロピーをもつ 3 値レスポンスを入力とするため，デバイアシング後のレスポンスの長さが向上する．

## 3.　評価実験

PUF のレスポンスを模して生成したランダムな 3 値の列に対してデバイアシングを適用し，レスポンスのバイアスやランダムセルの数を変化させた場合におけるデバイアシング後のレスポンスのバイアスとレスポンス長を評価する．ここで，PUF を構成するセル数は 1,024 個と仮定する．

図 1 に各条件下で (a) 既存の 2 値デバイアシング手法 [2]，(b) 提案する 3 値デバイアシング手法によってデバイアシング後のレスポンスを 1,000 回生成したときのデバイアシング後のレスポンスのバイアスの最悪値を表すカラーマップを示す．横軸は生成された PUF レスポンスのランダムセル数を表し，縦軸はレスポンスのバイアス（ランダムセルを除いたレスポンスにおける 0 の出現確率 $p_0$）を表す．デバイアシング後の出力ビット列のバイアス $p'_0$ がバイアスのないことを表す $|p'_0 - 0.5| = 0$ にどれだけ近いかを色を用いて表しており，青が濃い箇所ほど理想値に近く，赤い箇所ほどバイアスが大きいことを表す．提案手法は既存手法と比較して最悪値であってもバイアスの小さなレスポンスを抽出できることが確認できた．

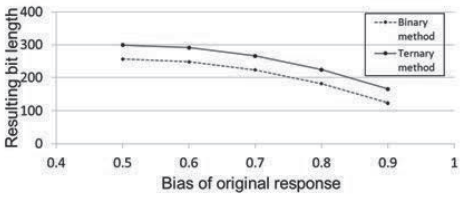


図 2　デバイアシング前のバイアスと各手法によって得られたビット数の関係

次に，図 2 にレスポンスのバイアスを変化させたときの各デバイアシング手法に基づくデバイアシングによって得られたデバイアシング後のレスポンスのビット長を示す．どの条件下においても提案手法の方が既存手法よりもデバイアシング後のレスポンス長が長いことが確認できた．

## 4.　まとめ

PUF を用いた固有 ID の高効率な生成方法について述べた．特に，多値の PUF レスポンスに対応するデバイアシング手法を提案するとともに，提案手法によって得られるレスポンスのバイアスとレスポンス長についての評価実験の結果を示し，提案手法によって高効率に PUF から固有 ID を抽出可能であることを示した．

## 文献

1) Y. Dodis, M. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” *SIAM J.Comput*, pp. 97–139, 2008.
2) R. Maes, V. van der Leest, E. van der Sluis, and F. Willems, “Secure key generation from biased PUFs,” *Cryptographic Hardware and Embedded Systems (CHES)*, pp. 517–534, 2015.
3) D. Yamamoto, K. Sakiyama, M. Iwamoto, K. Ohta, M. Takenaka, K. Itoh, and N. Torii, “A new method for enhancing variety and maintaining reliability of PUF responses and its evaluation on ASICs,” *Journal of Cryptographic Engineering*, pp. 187–199, 2015.